UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/863,199	05/21/2001	Stephen P. Weeks	7451.0034-00	8932

22852 7590 06/14/2006

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER LLP
901 NEW YORK AVENUE, NW
WASHINGTON, DC 20001-4413

EXAMINER	
TRUONG, THANHNGA B	
ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 06/14/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/863,199	WEEKS ET AL.	
	Examiner	Art Unit	
	Thanhnga B. Truong	2135	

-- Th MAILING DATE of this communication appears on the cov r sheet with th correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *4/3/2006 (RCE)*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-17* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-17* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *21 May 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on April 03, 2006 has been entered. Claims 1-17 are pending. At this time, claims 1-17 are rejected.

Claim Objections

2. Claims 1, 6-7, 9, and 11-12 are objected to because of the following informalities:

a. *Referring to claim 1:*

i. Applicant discloses in the third limitation of claim 1 "identifying a set of principals associated with **the computer-readable authorization certificates**". However, the second limitation of claim 1 recites "retrieving **a group of computer-readable authorization certificates** from at least one computer-readable authorization certificate storage location accessible to said computer-implemented authorization management system". The phrase **the group of computer-readable authorization certificates** should be used throughout the body of claim in order to be in consistence with the second limitation's language of claim 1. Furthermore, applicant discloses in the fourth limitation of claim 1 "creating **a lattice of authorization values** associated with each principal of said set of principals in a memory device in communication with the computer-implemented authorization system, wherein said **authorization values** are a monotone function of the authorizations of the set of principals". The phrase **the lattice of authorization values** should be used in "wherein said **authorization values** are a monotone function of the authorizations of the set of principals" in stead of **authorization values.** Appropriate correction is required.

b. *Referring to claim 6:*

i. Applicant discloses "in which **the request** is to access to a piece of electronic content; use a computer program; execute a transaction; access to a computer; or access to a network". Since this phrase of "**an electronic request**" has already been introduced in claim 1, **the electronic request** should be used instead. Appropriate correction is required.

c. *Referring to claim 7:*

i. Applicant discloses in the second limitation of claim 7 "computer code for retrieving **a group of computer-readable authorizations** for the predefined action". However, the third limitation of claim 7 only recites "computer code for identifying a set of principals associates with the **authorizations**". The phrase **the group of computer-readable authorizations** should be used in place of **authorizations** throughout the body of claim in order to be in consistence with the second limitation's language of claim 7. Similarly to the fourth limitation of claim 7 in which the claim recites "computer code for evaluating **authorizations** from the set of **authorizations** using the authorization value associated with each principal". The phrase **the group of computer-readable authorizations** should be used in place of **authorizations** throughout the body of claim in order to be in consistence with the second limitation's language of claim 7. Also the fourth limitation of claim 7 recites the phrase "**the authorization value"**, which has never been introduced in claim 7. Therefore, "**an authorization value"** should be used instead. The fifth limitation of claim 7 further recites "computer code for updating the authorization value of **the principals**". Since **"a set of principals"** has been introduced in the third limitation of claim 7, the phrase **"the set of principals"** should be used in the fifth limitation of claim 7. Similar rejection is applied to the sixth limitation of claim 7 for the terms **"authorizations"** and **"the principals"**. Appropriate correction is required.

d. *Referring to claim 9:*

i. Applicant discloses in the last limitation of claim 9 "means for granting the requesting principal access to the electronic content or processing resource". However, the fourth limitation of claim 9 recites "the requesting principal to access the piece of electronic content or processing resource". The phrase "the

requesting principal to access the piece of electronic content or processing resource" should be used throughout the body of claim in order to be in consistence with the first limitation's language of claim 9. Appropriate correction is required.

e. *Referring to claim 11:*

i. Applicant discloses "a second computer system for making a request for **system resources** from the first computer system". However, the fourth limitation of claim 10 recites **"computer-controlled electronic resources"**. The phrase **"computer-controlled electronic resources"** should be used throughout the body of claim in order to be in consistence with the limitation's language of claim 10. Appropriate correction is required.

f. *Referring to claim 12:*

i. Applicant discloses **"a monotone function"**. Since **"a monotone function"** has been introduced in claim 11, the phrase **"the monotone function"** should be used in claim 12. Appropriate correction is required.

Applicant is reminded to check for the same objection matter throughout the entire claims as well as other typographical errors and correct them appropriately.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Butt et al (US 6,754,829), and further in view of Kurshan (US 6,591,231).

a. *Referring to claim 1:*

i. Butt teaches in a computer-implemented authorization management system, a method for controlling a user's access to a computing resource

that is managed by said computer-implemented authorization management system (column 2, lines 26-40 of Butt), the method including:

(1) receiving an electronic request for the computing resource; retrieving a group of computer-readable authorization certificates from at least one computer-readable authorization certificate storage location accessible to said computer-implemented authorization management system, each certificate containing at least one computer-readable authorization by at least one principal **[i.e., Figure 6 is a flowchart for a manageable device testing a request received from a console operator. At this point, a console operator has already contacted a core, proven identity (e.g., by the core checking the operator's login identity on the operator's console), and received a signed certificate allowing the operator to communicate with a particular manageable device. A manageable device receives 300 the request along with a session certificate (column 10, lines 15-65 of Butt). In addition, allowing per-machine access control list granularity is beneficial, since operators are prevented from obtaining global access to all machines. That is, if authorizations were stored in the certificate, then an operator that has the right to perform a particular operation could perform this particular operation on any device-regardless of permachine policies (column 4, lines 52-57 of Butt). Furthermore, program modules include procedures, functions, programs, components, data structures, and the like, that perform particular tasks or implement particular abstract data types. The modules may be incorporated into single and multi-processor computing systems, as well as hand-held devices and controllable consumer devices. It is understood that modules may be implemented on a single computing device, or processed over a distributed network environment, where modules can be located in both local and remote memory storage devices (column 11, lines 58-67 of Butt)]**;

(2) identifying a set of principals associated with the computer-readable authorization certificates **[i.e., signing certificates (used by the certificate authority 104 to create session certificates) can be created by an outside entity, such as VeriSign Corporation, by the core itself, or by a second**

core, and then imported. No matter how the signing certificate is created, each manageable device must be pre-configured to trust the signing certificate. This can be done at manageable device installation time. By trusting a signing certificate, a manageable device is agreeing to trust any "session certificates" which are created by the owner of the "signing certificate." This means that a manageable device agrees to trust the authenticity of any console operators that contact it after logging into the core which owns the trusted "signing certificate." Associated with certificates are "public" and "private" keys, which are part of a "reversible" public-key encryption system, where data encrypted or signed with either key can be decoded or validated only with the other key. The public key is embedded within the certificate, and the private key is carefully stored and protected by the owner of the certificate (column 7, lines 1-19 of Butt)];

(3) creating a lattice of authorization values associated with each principal of said set of principals in a memory device in communication with the computer-implemented authorization system, wherein said authorization values are a monotone function of the authorizations of the set of principals; evaluating a certificate as a monotone function, at least in part, of the authorization value associated with one or more of the principals; updating the authorization value of one or more of the principals if the result of said evaluating step indicates that the authorization value of a principal should be changed; and repeating said evaluating and updating steps until a fixpoint of said lattice of authorization values is reached **[i.e., Figure 2 illustrates an authentication arrangement for one embodiment of the invention. Shown are a console computing device (console) 100, a core 102 computing device, a certificate authority (authority) 104, and a manageable device 106. Although only one manageable device 106 is illustrated, it is understood that many such will be present in a typical networked environment. The console is typically a computing device in use by an operator, where the operator seeks to manage the manageable device 106. The core 102 and certificate authority 104, as discussed below, allow the manageable device to validate the operator of the console, as well as any actions attempted by the operator. As illustrated, the core 102 and**

certificate authority 104 may be present within a single computing device, or they may be embodied in separate devices that are in communication with each other (column 5, lines 23-40). In addition, the core 102, by way of the certificate authority 104, issues operating system independent certificates to operators of consoles (e.g., console 100) which authenticate the identity of the console operators. As discussed above, the certificates embed a console operator's identity and group membership in the certificate, where access rights (in the form of access control lists) are stored at the manageable device(s) 106. The console operator proffers the certificate to a manageable device in support of a request to perform some management function. A manageable device 106, after receiving and validating the certificate, matches up the identity information within the certificate with the manageable device's local access control list information (column 5, lines 48-60)].

ii. Although Butt teaches certificate-based authentication system environments, Butt is silent on the capability of applying a fixpoint computation and a monotone function in their authorization management system. On the other hand, Kurshan teaches:

(1) The new formulation strengthens the Constructivity-FIX definition to require that every fixpoint of E* is .perp.-free. The equivalence of the two formulations is shown in Theorem 1. Definition 3 (Constructivity-SAT). A simultaneous definition (E,X,Y) is semantically acyclic iff (.A-inverted.v,u: .perp.free.v{character pullout}u=E*.(u,v):.perp.free.u). Lemma 0. For a monotone property P and a monotone function .function. on a CPO.OR right.,P.(lfp X:.function..X) iff (.A-inverted.u:u=.function..u:P.u). Proof. The implication form right to left is trivially true, as (l.function.X: .function..X) satisfies the condition u=.function..u. For the other direction, note that the fixpoints of fare partially ordered by .OR right., with the least fixpoint below any other fixpoint. By the monotonicity of P, if P holds for the least fixpoint, it holds for every fixpoint. Theorem 1. Constructivity-FIX and Constructivity-SAT are equivalent. Proof. For any simultaneous definition C=(E,X,Y), C satisfies Constructivity-FIX .congruent.(.A-inverted.v:.perp.free.v:.perp.free.(lfpY:E*.(v,Y))), by

definition .congruent.(.A-inverted.v:.perp.free.v:(.A-inverted.u:u=E*.(v,u): .perp.free.u)), by {.perp.free is monotone w.r.t .OR right.; Lemma 0} .congruent.(.A-inverted.v,u: .perp.free.v{character pullout}u=E*.(v,u):.perp.free.u), by rearranging .congruent.C satisfies Constructivity-SAT, by definition **(column 6, lines 30-56 of Kurshan).**

iii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) have modified the invention of Butt with the teaching of Kurshan to determine whether the authenticated operator has necessary access privilege to perform the management request based at least in part on the authenticated group membership of the operator set forth in the operating system independent session certificate **(column 1, lines x-x of Butt).**

iv. The ordinary skilled person would have been motivated to:

(1) have modified the invention of Butt with the teaching of Kurshan to providing remote-access to manageable devices across different operating systems, and more specifically, to using certificates with embedded cryptographic data to validate operator identity and access rights to remotely manageable devices **(column 1, lines x-x of Butt).**

b. *Referring to claim 2:*

i. The combination of teaching between Butt and Kurshan teaches:

(1) constructing a dependency graph representation in a memory device in communication with the computer-implemented authorization system, the dependency graph containing a node corresponding to each principal in the set of principals; and assigning at least two nodes in the dependency graph with a certificate that expresses a dependency of one node on the state of another node; wherein the dependency graph representation is used, at least in part, during said evaluating, updating, and repeating to determine which certificates to evaluate **[i.e., referring to Figure 7, this certificat is then marked 356 as a delegate certificate, and adds information in the additional information section of the certificate (see Figure 3) identifying the source of authority and delegation. The resulting session**

certificate can be used by the core to manage a manageable device 358 as session certificates would be used by a console operator. In addition, program modules include procedures, functions, programs, components, data structures, and the like, that perform particular tasks or implement particular abstract data types. The modules may be incorporated into single and multi-processor computing systems, as well as hand-held devices and controllable consumer devices. It is understood that modules may be implemented on a single computing device, or processed over a distributed network environment, where modules can be located in both local and remote memory storage devices (column 11, lines 43-67 of Butt). Moreover, Kurshan further teaches the dependency graph is met on column 1, lines 6-9 of Kurshan].

c. *Referring to claim 3:*

i. This claim has limitations that is similar to those of claim 1, thus it is rejected with the same rationale applied against claim 1 above.

d. *Referring to claim 4:*

i. This claim has limitations that is similar to those of claims 1-2, thus it is rejected with the same rationale applied against claims 1-2 above.

e. *Referring to claim 5:*

i. Butt further teaches:

(1) in which the certificates comprise Simple Public Key Infrastructure certificates **[i.e., referring to Figure 3, element 160 of Butt].**

f. *Referring to claim 6:*

i. Butt further teaches:

(1) in which the request is to access to a piece of electronic content; use a computer program; execute a transaction; access to a computer; or access to a network **[i.e., Figure 6 is a flowchart for a manageable device testing a request received from a console operator. At this point, a console operator has already contacted a core, proven identity (e.g., by the core checking the operator's login identity on the operator's console), and received a signed certificate allowing the operator to communicate with a particular**

manageable device. A manageable device receives 300 the request along with a session certificate (column 10, lines 15-65 of Butt). In addition, the operating system independent session certificate is provided by the operator to the device executing a third operating system, along with a management request. And, the device determines whether the authenticated operator has necessary access privilege to perform the management request based at least in part on the authenticated group membership of the operator set forth in the operating system independent session certificate (column 2, lines 33-40 of Butt - summary)].

g. *Referring to claim 7:*

i. This claim consists a computer program product for making trust management determinations to implement claim 1 and is rejected with the same rationale applied against claim 1 above, wherein the limitation of a computer-readable medium for storing the computer codes is disclosed in Figure 8, element 408, element 410, element 442, and element 444 (see also column 12, lines 13-18 of Butt).

h. *Referring to claim 8:*

i. Butt further teaches:

(1) in which the computer readable medium is one of: CD-ROM, DVD, MINIDISC, floppy disk, magnetic tape, flash memory, ROM, RAM, system memory, network server, hard drive, and optical storage **[i.e., referring to Figure 8, element 408, element 410, element 442, and element 444 (see also column 11, lines 58-67). Furthermore, the storage systems and associated computer-readable media provide storage of data and executable instructions for the computing device 402. Note that storage options include hard-drives, floppy-disks, optical storage, magnetic cassettes, tapes, flash memory cards, memory sticks, digital video disks, and the like (column 12, lines 13-18 of Butt)].**

i. *Referring to claim 9:*

i. This claim consists a system for controlling access to electronic content or processing resources to implement claim 1 and is rejected with the same rationale applied against claim 9 above.

ii. Butt further teaches:

(1) means for granting the requesting principal access to the electronic content or processing resource when the least fixpoint computation indicates that the root principal has authorized said access **[i.e., the operating system independent session certificate is provided by the operator to the device executing a third operating system, along with a management request. And, the device determines whether the authenticated operator has necessary access privilege to perform the management request based at least in part on the authenticated group membership of the operator set forth in the operating system independent session certificate (column 2, lines 33-40 of Butt - summary)]**.

j. *Referring to claim 10:*

i. Butt teaches a computer-implemented system for controlling access to computer-control electronic resources (column 2, lines 26-40 of Butt), the system comprising:

(1) a first computer system for processing electronic requests for access to computer-controlled electronic resources, the first computer system comprising: a computer network interface configured to receive digital certificates from other computer systems and for electronically receiving and processing requests to access electronic resources; a memory device in communication with said first computer system for storing electronic resources and one or more computer-readable authorization certificates relating to authorization for controlling access thereto **[i.e., referring to Figure 8, an exemplary system for implementing the invention includes a computing device 402 having system bus 404 for coupling together various components within the computing device. The system 404 bus may be any of several types of bus structures, such as PCI, AGP, VESA, Microchannel, ISA and EISA, etc. Typically, attached to the bus 402 are processors 406 such as Intel, DEC Alpha, PowerPC, programmable gate arrays, etc., a memory 408 (e.g., RAM, ROM), storage devices 410, a video interface 416, input/output interface ports 418, and a network interface 420. It is understood that a modem 448 may operate in conjunction with an input port 418 to operate an alternative network interface. The storage systems and associated computer-readable media provide**

storage of data and executable instructions for the computing device 402. Note that storage options include hard-drives, floppy-disks, optical storage, magnetic cassettes, tapes, flash memory cards, memory sticks, digital video disks, and the like (column 12, lines 1-18 of Butt)]; and

(2) a trust management engine for processing digital certificates and requests for electronic resources, and for making access control decisions by creating a lattice of monotone authorization values in a memory device associated with in a memory device in communication with said system and performing least fixpoint computations using said authorization values **[i.e., referring to Figure 6, The manageable device then verifies 302 that a trusted certificate authority associated with a core has signed the session certificate. Verification can be accomplished by using the issuer fields in the session certificate to lookup the certificate authority's certificate and verify that the session certificate was signed by the private key of the certificate authority (the core). Signature validation can be accomplished through application of known hash-check analysis on the signature, or by other techniques according to the nature of the signature. If 304 signature validation fails, then the manageable device ignores 306 all requests from the console. In one embodiment, the manageable device also sends an intruder detection warning to the core (column 10, lines 23-65 of Butt)].**

ii. Although Butt teaches certificate-based authentication system environments, Butt is silent on the capability of applying a fixpoint computation in their authorization management system. On the other hand, Kurshan teaches:

(1) The new formulation strengthens the Constructivity-FIX definition to require that every fixpoint of E* is .perp.-free. The equivalence of the two formulations is shown in Theorem 1. Definition 3 (Constructivity-SAT). A simultaneous definition (E,X,Y) is semantically acyclic iff (.A-inverted.v,u: .perp.free.v{character pullout}u=E*.(u,v):.perp.free.u). Lemma 0. For a monotone property P and a monotone function .function. on a CPO.OR right.,P.(lfp X:.function..X) iff (.A-inverted.u:u=.function..u:P.u). Proof. The implication form right to left is trivially true, as (l.function.X: .function..X) satisfies the condition u=.function..u. For the other

direction, note that the fixpoints of fare partially ordered by .OR right., with the least fixpoint below any other fixpoint. By the monotonicity of P, if P holds for the least fixpoint, it holds for every fixpoint. Theorem 1. Constructivity-FIX and Constructivity-SAT are equivalent. Proof. For any simultaneous definition C=(E,X,Y), C satisfies Constructivity-FIX .congruent.(.A-inverted.v:.perp.free.v:.perp.free.(lfpY:E*.(v,Y))), by definition .congruent.(.A-inverted.v:.perp.free.v:(.A-inverted.u:u=E*.(v,u): .perp.free.u)), by {.perp.free is monotone w.r.t .OR right.; Lemma 0} .congruent.(.A-inverted.v,u: .perp.free.v{character pullout}u=E*.(v,u):.perp.free.u), by rearranging .congruent.C satisfies Constructivity-SAT, by definition **(column 6, lines 30-56 of Kurshan).**

iii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) have modified the invention of Butt with the teaching of Kurshan to determine whether the authenticated operator has necessary access privilege to perform the management request based at least in part on the authenticated group membership of the operator set forth in the operating system independent session certificate **(column 1, lines x-x of Butt).**

iv. The ordinary skilled person would have been motivated to:

(1) have modified the invention of Butt with the teaching of Kurshan to providing remote-access to manageable devices across different operating systems, and more specifically, to using certificates with embedded cryptographic data to validate operator identity and access rights to remotely manageable devices **(column 1, lines x-x of Butt).**

k. *Referring to claim 11:*

i. Butt further teaches:

(1) a second computer system for making a request for system resources from the first computer system; a third computer system for generating a first digital certificate, the first digital certificate including an authorization value that is generated from a monotone function, the authorization value effective for authorizing, at least in part, the second computer system to access a predefined system resource **[i.e., referring to Figure 8, it is understood that a remote computing**

device can be configured like computing device 402, and therefore may include many or all of the elements discussed for computing device 402. It should also be appreciated that remote computing devices 442 may be embodied separately, or combined within a single device; for example, a core and certificate authority may be combined into a single device which coordinates a console operator's access to a particular manageable device (column 12, lines 36-45 Butt)].

l. *Referring to claims 12, 13:*

i. These claims consist additional system for controlling access to electronic content or processing resources to implement claim 11 and is rejected with the same rationale applied against claim 11 above.

m. *Referring to claim 14:*

i. Butt further teaches:

(1) in which the first computer system further comprises a public key stored in a memory device in communication with said first computer system and associated with the fourth computer system, the public key corresponding to a private key used to sign the second digital certificate **[i.e. referring to Figure 3, element 160 and element 352 of Figure 7. In addition, the manageable device can also verify that the console operator has the private key associated with the public key embedded within the received session certificate (column 10, lines 36-39 of Butt)].**

n. *Referring to claims 15-16:*

i. These claims have limitations that is similar to those of claim 5, thus they are rejected with the same rationale applied against claim 5 above.

o. *Referring to claim 17:*

i. This claim consists a computer-implemented method for performing authorization management computations using a computer system to implement claim 10 and is rejected with the same rationale applied against claim 10 above.

Conclusion

5. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 571-272-3858.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The central fax number for the organization where this application or proceeding is assigned is **571-273-8300.**

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

Thanhnga B. Truong

TBT
June 08, 2006